P.O. Box 30285
Salt Lake City, UT 84130-0285

September 11, 2019

Attorney General's Office
California Department of Justice
P.O. Box 944255
Sacramento, CA 94244-2550

Dear Attorney General Xavier Becerra:

This is an update to the data security event that we previously notified you about on August 12, 2019.

As indicated previously, after receiving a referral from an external security researcher, we determined on July 19, 2019 that there was unauthorized access on March 22 and March 23, 2019 by an outside individual who obtained certain types of personal information relating to people who had applied for a Capital One credit card product and existing Capital One credit card customers. After finding out about the issue, Capital One promptly took action by fixing it, verifying that there are no other instances of the vulnerability in our environment, and commencing an investigation.

We believe it is unlikely that the information was used for fraud or disseminated by the individual, who has been arrested for her conduct. Credit card account number(s) and log-in credentials were not compromised.

The largest category of information accessed was information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019. This information included names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income. The individual also obtained portions of credit card customer data, including customer status data (for example, credit scores, credit limits, balances, payment history, contact information) and fragments of transaction data from a total of 23 days during 2016, 2017 and 2018.

In addition, for a subset of these consumers, about 140,000 Social Security Numbers and 80,000 linked bank account numbers were obtained.

Capital One mailed a written notice to the impacted California residents pursuant to the Security Breach Notice Act, Cal. Civ. Code §1798.82. Beginning August 8 and ending August 30, we have mailed notice to a total of twenty five thousand eight hundred and fifty (25,850) residents of your state that their Social Security number and/or Bank Account Number(s) may have been obtained in the incident. In order to mitigate the risk of identity theft associated with this incident, we are providing free access to two years of credit monitoring services through the "*my*TrueIdentity" services product offered by TransUnion to the impacted California residents. This notice does not include information pertaining to remailed breach notices resulting from returned mail. At this time, we have no reason to believe this number of impacted residents will change.

We have attached an example of the customer notifications, which vary based on each customer's particular circumstance.

We remain committed to maintaining high standards for customer service and customer data security and want to assure you that we are taking appropriate steps to protect the personal information of our customers.

If you have any questions, comments or concerns, please contact Jonathan Olin, Senior Associate General Counsel at (202) 596-5804 or Jonathan.Olin@capitalone.com.

Sincerely,

Ryan D. Barker
Senior Director, Privacy Office

P.O. Box 85619
Richmond, VA 23285-5619

[redacted]

August 24, 2019

RE: Bank account ending in [redacted]
Case No. DSE 191404

NOTICE OF DATA BREACH

Dear [redacted],

We are writing to notify you of a Capital One® data security incident that involves your personal information that was provided to us as part of a credit card application. Capital One is committed to safeguarding your data, and we are deeply sorry for this situation and the understandable worry it must be causing you. This letter explains what happened based on our analysis to date, what you can do in response, and what we are doing to make this right.

WHAT HAPPENED
On July 19, 2019, Capital One determined that an individual outside of Capital One gained unauthorized access to and obtained certain types of personal information about our credit card customers and people who have applied for our credit cards. This occurred on March 22 and 23, 2019.

WHAT INFORMATION WAS INVOLVED
The personal information obtained by the individual included your name and the bank account number referenced above. This information was provided to Capital One by someone applying for one of Capital One's secured card accounts, as a source of funding for the associated account deposit.

We believe it is unlikely that the information was used for fraud or disseminated by the individual, who has been arrested for her conduct. Credit card account numbers and log-in credentials were not compromised.

WHAT ARE WE DOING
As a precaution, we're offering you two years of credit monitoring and identity protection with TransUnion's credit monitoring service at no cost to you. You can sign up for this service by using the enclosed code and instructions any time before December 02, 2019. Due to privacy laws, we cannot register you directly. This service will not auto-renew.

Additionally, we want to let you know that upon learning of the incident, Capital One immediately fixed the issue and promptly began working with federal law enforcement. We have invested heavily in cybersecurity and will continue to do so, and we will use what we've learned from this incident to further strengthen our cyber defenses.

WHAT YOU CAN DO
In addition to your enrolling in the credit monitoring service, we've included a list of resources for protecting yourself against potential misuse of your personal information.

FOR MORE INFORMATION
Once again, we sincerely apologize. We want you to know that we are here for you and welcome any questions. We've set up a dedicated website at www.capitalone.com/facts2019. We also invite you to call us at 1-844-388-8999. Our dedicated support team for this incident is standing by to answer your questions and care for your needs 24/7.

Sincerely,

Capital One

HOW TO ENROLL IN CREDIT MONITORING

As noted above, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (*my*TrueIdentity) for two years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting agencies.

- To enroll in this service, go to the *my*TrueIdentity website at **www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code** [redacted] and follow the three steps to receive your credit monitoring service online within minutes.

- If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code [redacted] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft. TransUnion representatives are available Monday-Friday, 8 a.m.-8 p.m. ET.

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. The three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian®, and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

- You can sign up for the online or offline credit monitoring service anytime between now and **December 02, 2019**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, Experian, or Equifax, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

- **Special note for minors affected by this incident:** The same services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if your child may be a victim of identity theft by using TransUnion's secure online form at www.transunion.com/childidentitytheft to submit your information so TransUnion can check their database for a credit file with your child's Social Security number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this fraudulent activity.

ADDITIONAL RESOURCES

You should remain vigilant for instances of fraud or identity theft over the next 12 to 24 months by reviewing your account statements and closely monitoring your credit reports, which are available to you free of charge. You may obtain a free copy of your credit report once every 12 months from each of the three nationwide credit reporting agencies. Contact information for these agencies is as follows:

Equifax:	**Experian**:	**TransUnion:**
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

Annual Credit Report. You may order a free annual credit report. To do so, please visit www.annualcreditreport.com or call 1-877-322-8228.

You can also order your free annual credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by contacting one of the three nationwide credit reporting agencies listed above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or make certain changes to your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report. A security freeze will prevent a credit reporting agency from releasing information in your credit report without your express authorization. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the credit reporting agency certain identifying information, including your full name; Social Security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or insurance statement. Under the Economic Growth, Regulatory Relief, and Consumer Protection Act, you have the right to place a security freeze on your account free of charge.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
http://www.marylandattorneygeneral.gov/
1-888-743-0023

North Carolina Office of the Attorney General
Mail Service Center 9001
Raleigh, NC 27699-9001
http://www.ncdoj.gov/
1-877-566-7226

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
401-274-4400

Reporting identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.	**For Massachusetts residents:** You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.	**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.	**For Rhode Island residents:** You have the right to file or obtain a police report regarding this incident.

Federal Fair Credit Reporting Act Rights: The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how credit reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of credit reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; credit reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; credit reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

P.O. Box 85619
Richmond, VA 23285-5619

[redacted]

August 29, 2019

Case No. DSE 191404

NOTICE OF DATA BREACH

Dear [redacted],

We are writing to notify you of a Capital One® data security incident that involves your personal information. Capital One is committed to safeguarding your data, and we are deeply sorry for this situation and the understandable worry it must be causing you. This letter explains what happened based on our analysis to date, what you can do in response, and what we are doing to make this right.

WHAT HAPPENED

On July 19, 2019, Capital One determined that an individual outside of Capital One gained unauthorized access to and obtained certain types of personal information about our credit card customers and people who have applied for our credit cards. This occurred on March 22 and 23, 2019.

We believe it is unlikely that the information was used for fraud or disseminated by the individual, who has been arrested for her conduct. Credit card account numbers and log-in credentials were not compromised.

The largest category of information accessed was information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019. This information included names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income. The individual also obtained portions of credit card customer data, including customer status data (for example, credit scores, credit limits, balances, payment history, and contact information) and fragments of transaction data from a total of 23 days during 2016, 2017 and 2018.

In addition, for a subset of these consumers, about 140,000 Social Security numbers and 80,000 linked bank account numbers were obtained. We are sorry that your Social Security number was one of the 140,000 obtained.

WHAT INFORMATION WAS INVOLVED

The personal information obtained by the individual included your name, Social Security number and also may have included date of birth, contact information, and other customer and credit data as described above.

WHAT ARE WE DOING

As a precaution, we're offering you two years of credit monitoring and identity protection with TransUnion's credit monitoring service at no cost to you. You can sign up for this service by using the enclosed code and instructions any time before December 07, 2019. Due to privacy laws, we cannot register you directly. This service will not auto-renew.

Additionally, we want to let you know that upon learning of the incident, Capital One immediately fixed the issue and promptly began working with federal law enforcement. We have invested heavily in cybersecurity and will continue to do so, and we will use what we've learned from this incident to further strengthen our cyber defenses.

WHAT YOU CAN DO

In addition to your enrolling in the credit monitoring service, we've included a list of resources for protecting yourself against potential misuse of your personal information.

FOR MORE INFORMATION

Once again, we sincerely apologize. We want you to know that we are here for you and welcome any questions. We've set up a dedicated website at www.capitalone.com/facts2019. We also invite you to call us at 1-844-388-8999. Our dedicated support team for this incident is standing by to answer your questions and care for your needs 24/7.

Sincerely,

Capital One

HOW TO ENROLL IN CREDIT MONITORING

As noted above, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (*my*TrueIdentity) for two years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting agencies.

- To enroll in this service, go to the *my*TrueIdentity website at **www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code** [redacted] and follow the three steps to receive your credit monitoring service online within minutes.

- If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code [redacted] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft. TransUnion representatives are available Monday-Friday, 8 a.m.-8 p.m. ET.

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. The three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian®, and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

- You can sign up for the online or offline credit monitoring service anytime between now and **December 07, 2019**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, Experian, or Equifax, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

- **Special note for minors affected by this incident:** The same services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if your child may be a victim of identity theft by using TransUnion's secure online form at www.transunion.com/childidentitytheft to submit your information so TransUnion can check their database for a credit file with your child's Social Security number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this fraudulent activity.

ADDITIONAL RESOURCES

You should remain vigilant for instances of fraud or identity theft over the next 12 to 24 months by reviewing your account statements and closely monitoring your credit reports, which are available to you free of charge. You may obtain a free copy of your credit report once every 12 months from each of the three nationwide credit reporting agencies. Contact information for these agencies is as follows:

Equifax:	**Experian**:	**TransUnion:**
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

Annual Credit Report. You may order a free annual credit report. To do so, please visit www.annualcreditreport.com or call 1-877-322-8228.

You can also order your free annual credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by contacting one of the three nationwide credit reporting agencies listed above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or make certain changes to your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report. A security freeze will prevent a credit reporting agency from releasing information in your credit report without your express authorization. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the credit reporting agency certain identifying information, including your full name; Social Security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or insurance statement. Under the Economic Growth, Regulatory Relief, and Consumer Protection Act, you have the right to place a security freeze on your account free of charge.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
http://www.marylandattorneygeneral.gov/
1-888-743-0023

North Carolina Office of the Attorney General
Mail Service Center 9001
Raleigh, NC 27699-9001
http://www.ncdoj.gov/
1-877-566-7226

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
401-274-4400

Reporting identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.	**For Massachusetts residents:** You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.	**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.	**For Rhode Island residents:** You have the right to file or obtain a police report regarding this incident.

Federal Fair Credit Reporting Act Rights: The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how credit reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of credit reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; credit reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; credit reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.